| NODIS Library | Legal Policies(2000s) | Search |

NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2016

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)

Responsible Office: Office of the Chief Information Officer

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | ALL |

Preface

P.1 Purpose

The purpose of this document is to:

a. Establish the information security requirements for the National Aeronautics and Space Administration (NASA) relative to the policy set forth in NASA Policy Directive (NPD) 2810.1, NASA Information Security Program. The procedural requirements, herein prescribe roles, responsibilities, and conditions that directly or indirectly promote information security throughout the life cycle of all NASA information and information systems.

b. Identify information security policies, procedures, and practices which are appropriate to NASA's mission, and are consistent with applicable federal laws, executive orders, directives, policies, and regulations.

c. Serve as a reference to the NASA community regarding specific information security roles and responsibilities, and provide resources where more detailed information may be found.

d. Satisfy security policy guidance as outlined by National Institute of Standards Technology (NIST), Special Publication (SP) 800-53. Recommended Security Controls for Federal Information Systems and Organizations.

P.2 Applicability

a. This NASA Procedural Requirement (NPR) applies to:

(1) NASA Headquarters and all NASA Centers, including Component Facilities and Technical and Service Support Centers.

(2) For purposes of this NPR, NASA Headquarters is treated as a Center. Further, all roles and responsibilities of a Center Chief Information Officer (CIO) are also applicable to the NASA Headquarters CIO and all stipulated Center requirements are also applicable to NASA Headquarters.

(3) NASA Jet Propulsion Laboratory (JPL), other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

(4) This NPR applies to unclassifieed NASA information and information systems, including those that are contracted out or outsourced to (1) a Government owned, contractor operated (GOCO) facility; (2) partners under the Space Act; (3) partners under the Commerical Space Act of 1997; or (4) commercial or university facilities.

(5) Information systems that do not process NASA information, or are merely incidental to a contract (e.g., a contractor's payroll and personnel management system) are normally excluded from full review or audits, to protect proprietary and private data.

(6) This NPR does not apply to Classfied National Security Information (CNSI). CNSI is the responsibility of the Office of Protective Services and is coverned under CNSI policy and requirements contained in NPD 1600.2, NASA Security Policy and NPR 1600.1, NASA Security Program Procedural Requirements.

P.3 Authority

a. 5 U.S.C. § 552, et seq., the Freedom of Information Act, as implemented by 14 C.F.R.§ 1206, Availability of Agency Records to Members of the Public, as amended.

b. 5 U.S.C. § 552a, the Privacy Act, Pub. L. No. 93-579.

c. 5 U.S.C. App. III, Inspector General Act of 1978.

d. 18 U.S.C. § 799, Violation of Regulations of National Aeronautics and Space Administration, as amended.

e. 18 U.S.C. § 2510, et seq., Electronic Communications Privacy Act of 1986, as amended.

f. 22 U.S.C. § 2751, et seq., Arms Export Control Act, as implemented by 22 C.F.R. § 120-130, International Traffic in Arms Regulations.

g. 40 U.S.C. § 11101 et seq., Chapter 808 of Pub. L 104-208, the Clinger-Cohen Act of 1996.

h. 42 U.S.C. § 201 nt., Health Insurance Portability and Accountability Act of 1996, as amended.

i. 44 U.S.C. § 101, E-Government Act of 2002.

j. 44 U.S.C. § 3535, Federal Information Security Management Act (FISMA) of 2002.

k. 44 U.S.C. § 3501, et seq., Paperwork Reduction Act of 1995, as amended.

l. 50 U.S.C. Appendix 2401-2420, Export Administration Act of 1979, as amended.

m. 51 U.S.C. § 20113(e), The National Aeronautics and Space Act of 1958, as amended.

n. EO 12958, Classified National Security Information, dated April 17, 1992.

o. EO 13011, Federal Information Technology, dated July 16, 1996.

p. 14 C.F.R § 1206, Availability of Agency Records to Members of the Public.

q. 15 C.F.R § 730-774, Export Administration Regulations.

r. 22 C.F.R § 120-130, International Traffic in Arms Regulations.

P.4 Applicable Documents

a. FIPS 140, Security Requirements for Cryptographic Modules.

b. FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

c. HSPD-12, Policies for a Common Identification Standard for Federal Employees and Contractors, August 2004.

d. HSPD-20, National Continuity Policy.

e. NIST SP 800-30, Risk Management Guide for Information Technology Systems.

f. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

g. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.

h. NIST SP 800-46, Guide to Enterprise Telework and Remote Access Security.

i. NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations.

j. NIST SP 800-61, Computer Security Incident Handling Guide.

k. NIST SP 800-63, Electronic Authentication Guideline.

l. NIST SP 800-83, Guide to Malware Incident Prevention and Handling.

m. NIST SP 800-88, Guidelines for Media Sanitization.

n. NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

o. X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

p. NPD 1600.2, NASA Security Policy.

q. NPD 1600.3, Policy on Prevention of and Response to Workplace Violence.

r. NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology.

s. NPD 2810.1, NASA Information Security Policy.

t. NPR 1040.1, NASA Continuity of Operations Planning (COOP) Procedural Requirements.

u. NPR 1382.1, NASA Privacy Procedural Requirements.

v. NPR 1441.1, NASA Records and Retention Schedule.

w. NPR 1600.1, NASA Security Program Procedural Requirements.

x. NPR 1620.2, Physical Security Vulnerability Risk Assessments.

y. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

z. NPR 2800.1, Managing Information Technology.

aa. NPR 2841.1, Identity, Credential, and Access Management Services.

bb. NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.

cc. NPR 8000.4, Agency Risk Management Procedural Requirements.

dd. NPR 8820, Facility Project Requirements.

ee. NPR 8831.2, Facilities Maintenance and Operations Management.

ff. ITS-HBK-2841-001, Identity, Credential, and Access Management (ICAM) Services Handbook.

gg. ITS-HBK-2810-02, Security Assessment and Authorization.

hh. ITS-HBK-2810-03, Planning.

ii. ITS-HBK-2810-04, Risk Assessment.

jj. ITS-HBK-2810-05, System and Services Acquisition.

kk. ITS-HBK-2810-06, Security Awareness and Training.

ll. ITS-HBK-2810-07, Configuration Management.

mm. ITS-HBK-2810-08, Contingency Planning.

nn. ITS-HBK-2810-09, Incident Response and Management.

oo. ITS-HBK-2810-10, Maintenance.

pp. ITS-HBK-2810-11, Media Protection.

qq. ITS-HBK-2810-12, Physical and Environmental Protection.

rr. ITS-HBK-2810-13, Personnel Security.

ss. ITS-HBK-2810-14, System and Information Integrity.

tt. ITS-HBK-2810-15, Access Control.

uu. ITS-HBK-2810-16, Audit and Accountability.

vv. ITS-HBK-2810-17, Identification and Authentication.

ww. ITS-HBK-2810-18, System and Communication.

P.5 Measurement/Verification

a. The obligation to measure performance and reduce cost is driven by Federal regulatory and NASA requirements. These measurements shall be based upon NASA's goals and objectives, be designed to provide substantive justification for decision-making, and be utilized to measure the effectiveness of the information security program, policies, and requirements. Information security program measurement goals and objectives are not static and will be adjusted as the operating environment, threats, and requirements evolve.

b. The Office of the CIO shall provide assessments/audits of the application of this NPR. This will consist of periodic reporting from the Centers, including information collected for the satisfaction of Office of Management and Budget (OMB) and the Federal Information Security Management Act (FISMA) reporting requirements.

c. All covered entities are subject to information security compliance reviews and audits by NASA.

P.6 Cancellation

a. NPR 2810.1, Security of Information Technology, August 12, 2004

b. NITR-2810-12, Continuous Monitoring, May 18, 2008

c. NITR-2810-14, Managing Elevated User Privileges on NASA IT Devices, August 17, 2009

d. NITR-2810-15, Contingency Planning, June 9, 2008

e. NITR-2810-17, System Maintenance Policy and Procedures, November 12, 2008

f. NITR-2810-19, Audit and Accountability Policy and Procedures, November 12, 2008

g. NITR-2810-20, System and Communications Protection Policy and Procedures, March 11, 2009

h. NITR-2810-21, System and Services Acquisition Policy and Procedures, April 28, 2009

i. NITR-2810-22, Media Protection Policy and Procedures, January 7, 2009

j. NITR-2810-23, NASA Authorizing Official (AO) Procedural Requirements, March 1, 2009

k. NITR-2810-24, NASA IT Device Vulnerability Management, January 28, 2010

Revalidated May 19, 2011, Orginal signed by:

/S/
Patricia Dunnington
Chief Information Officer

DISTRIBUTION: NODIS

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS
